S2SCHOOL

Zoom Security Best Practices

Cybersecurity @Home

5509 Baker Road, Suite 500
Minnetonka, MN 55345

securitystudio.com
info@securitystudio.com

Zoom Security Best Practices

In our new world of 100% remote learning, data privacy, and security concerns require heightened levels of attention from all of us. The following protocols are intended to guide our practices in a way supportive of strong data privacy and digital security.

"Zoom Bombing" is occurring in many virtual classrooms across the country; this is when a stranger joins a virtual meeting and shares pornographic images, or uses threatening or hate language.

Please carefully review the considerations below and adjust accordingly.

Video Conferencing - Data Privacy and Security Considerations

- Do not post screenshots of video meeting participants on social media. This goes for both classroom meetings and staff only meetings.
- Be aware of what is in your camera background; do not overshare personal information.
- Close all unnecessary windows before sharing your desktop to avoid accidentally showing sensitive emails or other information.
- For the safety of both students and teachers, video conferencing must not be used for one-on-one communication between students and teachers.
    - If this is necessary for special education or other student services, please contact Special Education team to discuss; parental consent may be required.
- Teachers should not record live video conferences. Teachers may record other instructional material or non-live lectures and post for students to view.
- Do not make meetings or classrooms publicly accessible.
- Do not post links to video conferences on any public website.
- Conduct video conferences during school hours.
- Students from outside of our district should not be allowed to join a video conference.
- The teacher must always be the last person to hang up and end the video conference.
- Like at school, be explicit with students about behavior and expectations on video conferencing. For example, clothing, background, and how to participate respectfully.
    - If there are students who join the group who are not dressed appropriately, the teacher should stop the video conference and contact the student's parents. For example: If a student joins the group with no shirt on, etc. Please avoid identifying the student or cause of the disruption to the rest of the attendees.
    - If a teacher witnesses something inappropriate in the background, the video conference should be stopped immediately and the parent should be called. Please avoid identifying the student or cause of the disruption to the rest of the attendees.

Please contact your building or district administration with any privacy concerns.

Video Conferencing - General Settings for Optimal Data Privacy and Security

- Set screen sharing to "Host-Only" to prohibit undesired participant sharing.
- Disable "Join Before Host" so participants can't enter the meeting early.
- Disable the ability for participants to privately chat with each other.
- Disable "File Transfer" so there's no digital virus sharing.
- Disable "Allow Removed Participants to Rejoin" so removed attendees can't slip back in.
- Enable "Mute Participants on Entry" to minimize distracting background noise.
- Enable "Only Authenticated Users Can Join Meetings" if possible.
- Add a "Co-Host" if you are working with another adult who can help moderate.
- Utilize the "Waiting Room" feature (activated by default) and set meeting passwords to control attendees.
- Read this: Best Practices for Securing Your Zoom Virtual Classroom for complete information on the above settings and more.
- These Tips & Tricks for Teachers Educating on Zoom are also available.

Cybersecurity is just as important while working from home, perhaps even more important. Email phishing attempts that can cause ransomware and other destruction are rampant. Rockford Public Schools suffered a debilitating and costly ransomware attack last fall; They are still recovering. The threat is real, potentially disastrous, and ever-present.

Please carefully review the considerations below and adjust accordingly.

Digital Security Considerations

- If you are using the district's VPN to access internal resources, please disconnect from the VPN as soon as you are finished. Open VPN connections are a security risk.
- Be particularly suspicious of ALL the emails you receive. Malicious breaches and attacks have skyrocketed as cybercriminals capitalize on our kind hearts and fears during this time.
  - Please review these email safety and security recommendations; they still hold true today. If you have ANY doubt, please delete the email!
- Please review these tips for digital safety while working from home, provided by a trusted security partner of ours.
  - If your home router needs updates, these tips will help.
  - Please consider taking this brief security assessment for important information on how you may improve the security of your new remote digital workspace (use your district email address to register.)
- Please review these tips for keeping your devices physically clean.
- For visual learners here is a how to video for securing zoom.

Please contact your building or district technology teams with any technical questions.